# Scan Report

May 22, 2025

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "myoppo.com". The scan started at Thu May 22 11:25:29 2025 UTC and ended at . The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

# Contents

# 1   Result Overview

| Host | High | Medium | Low | Log | False Positive |
|------|------|--------|-----|-----|----------------|
| 47.94.225.108 | 0 | 5 | 2 | 0 | 0 |
| 106.3.18.183 myoppo.com | 0 | 1 | 0 | 0 | 0 |
| Total: 2 | 0 | 6 | 2 | 0 | 0 |

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 8 results selected by the filtering described above. Before filtering there were 81 results.

# 2   Results per Host

## 2.1   47.94.225.108

Host scan start     Thu May 22 11:27:06 2025 UTC
Host scan end

| Service (Port) | Threat Level |
|----------------|--------------|
| 21/tcp | Medium |
| 22/tcp | Medium |
| general/icmp | Low |
| 22/tcp | Low |

### 2.1.1   Medium 21/tcp

| Medium (CVSS: 5.3) |
| NVT: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits |

**Summary**
The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.

. . . continues on next page . . .

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSL/TLS server is using the following certificate(s) with a RSA key w
↪ith less than 2048 bits (public-key-size:public-key-algorithm:serial:issuer):
1024:RSA:00CE0513A04300C81B:1.2.840.113549.1.9.1=#61646D696E4062742E636E,CN=47.9
↪4.225.108,OU=BT,O=BT-PANEL,L=Dongguan,ST=Guangdong,C=CN (Server certificate)

**Impact**
Using certificates with weak RSA key size can lead to unauthorized exposure of sensitive information.

**Solution:**
**Solution type:** Mitigation
Replace the certificate with a stronger key and reissue the certificates it signed.

**Vulnerability Insight**
SSL/TLS certificates using RSA keys with less than 2048 bits are considered unsafe.

**Vulnerability Detection Method**
Checks the RSA keys size of the server certificate and all certificates in chain for a size < 2048 bit.
Details: SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048.
↪..
OID:1.3.6.1.4.1.25623.1.0.150710
Version used: 2021-12-10T12:48:00Z

**References**
url: https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

---

**Medium (CVSS: 4.8)**
**NVT: FTP Unencrypted Cleartext Login**

**Summary**
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

**Quality of Detection (QoD):** 70%

**Vulnerability Detection Result**
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 User gbvt OK. Password required
Anonymous sessions:     331 User anonymous OK. Password required

```
The remote FTP service supports the 'AUTH TLS' command but isn't enforcing the u
↪se of it for:
- Non-anonymous sessions
- Anonymous sessions
```

**Impact**
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

**Solution:**
**Solution type:** Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual
of the FTP service for more information.

**Vulnerability Detection Method**
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command
first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS'
command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2023-12-20T05:05:58Z`

| Medium (CVSS: 4.0) |
| :--- |
| NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability |

**Summary**
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
`Server Temporary Key Size: 1024 bits`

**Impact**
An attacker might be able to decrypt the SSL/TLS communication offline.

**Solution:**
**Solution type:** Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-
Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which
include primes with lengths of more than 1024 bits.

**Vulnerability Insight**

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

**Vulnerability Detection Method**
Checks the DHE temporary public key size.
Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2024-09-30T08:38:05Z`

**References**
url: `https://weakdh.org/`
url: `https://weakdh.org/sysadmin.html`

[ return to 47.94.225.108 ]

### 2.1.2 Medium 22/tcp

**Medium (CVSS: 5.3)**
**NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)**

**Summary**
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                    | Reason
--------------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1        | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

**Impact**
An attacker can quickly break individual connections.

**Solution:**
**Solution type:** Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

**Vulnerability Insight**
- 1024-bit MODP group / prime KEX algorithms:
Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection-is dependent only on this prime.
A nation-state can break a 1024-bit prime.

**Vulnerability Detection Method**
Checks the supported KEX algorithms of the remote SSH server.
Currently weak KEX algorithms are defined as the following:
- non-elliptic-curve Diffie-Hellmann (DH) KEX algorithms with 1024-bit MODP group / prime
- ephemerally generated key exchange groups uses SHA-1
- using RSA 1024-bit modulus key
Details: `Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.150713
Version used: `2024-06-14T05:05:48Z`

**References**
url: `https://weakdh.org/sysadmin.html`
url: `https://www.rfc-editor.org/rfc/rfc9142`
url: `https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem`
url: `https://www.rfc-editor.org/rfc/rfc6194`
url: `https://www.rfc-editor.org/rfc/rfc4253#section-6.5`

| Medium (CVSS: 4.3) |
| --- |
| NVT: Weak Encryption Algorithm(s) Supported (SSH) |

**Summary**
The remote SSH server is configured to allow / support weak encryption algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
```
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
```

```
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
```

**Solution:**
**Solution type:** Mitigation
Disable the reported weak encryption algorithm(s).

**Vulnerability Insight**
- The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
- The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
- A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

**Vulnerability Detection Method**
Checks the supported encryption algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak encryption algorithms are defined as the following:
- Arcfour (RC4) cipher based algorithms
- 'none' algorithm
- CBC mode cipher based algorithms
Details: `Weak Encryption Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2024-06-14T05:05:48Z`

**References**
url: https://www.rfc-editor.org/rfc/rfc8758
url: https://www.kb.cert.org/vuls/id/958563
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.3

### 2.1.3   Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

**Summary**
The remote host responded to an ICMP timestamp request.

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0

**Impact**
This information could theoretically be used to exploit weak time-based random number generators in other services.

**Solution:**
**Solution type:** Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

**Vulnerability Insight**
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

**Vulnerability Detection Method**
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: ICMP Timestamp Reply Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2025-01-21T05:37:33Z

**References**
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

[ return to 47.94.225.108 ]

### 2.1.4   Low 22/tcp

| Low (CVSS: 2.6) |
| NVT: Weak MAC Algorithm(s) Supported (SSH) |

**Summary**

The remote SSH server is configured to allow / support weak MAC algorithm(s).

**Quality of Detection (QoD):** 80%

**Vulnerability Detection Result**
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com

**Solution:**
**Solution type:** Mitigation
Disable the reported weak MAC algorithm(s).

**Vulnerability Detection Method**
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH
server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

**References**
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

## 2.2   106.3.18.183

Host scan start    Thu May 22 11:27:06 2025 UTC
Host scan end      Thu May 22 12:39:00 2025 UTC

| Service (Port) | Threat Level |
| --- | --- |
| 443/tcp | Medium |

### 2.2.1   Medium 443/tcp

| |
|---|
| |

**Product detection result**
```
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

**Summary**
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

**Quality of Detection (QoD):** 98%

**Vulnerability Detection Result**
```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

**Impact**
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

**Solution:**
**Solution type:** Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

**Affected Software/OS**
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

**Vulnerability Insight**
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

**Vulnerability Detection Method**
Check the used TLS protocols of the services provided by this system.
Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.117274

Version used: 2024-09-27T05:05:23Z

**Product Detection Result**
Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

**References**
cve: `CVE-2011-3389`
cve: `CVE-2015-0204`
url: `https://ssl-config.mozilla.org/`
url: `https://bettercrypto.org/`
url: `https://datatracker.ietf.org/doc/rfc8996/`
url: `https://vnhacker.blogspot.com/2011/09/beast.html`
url: `https://web.archive.org/web/20201108095603/https://censys.io/blog/freak`
url: `https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters`
↪`-report-2014`
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441

| |
|---|
| dfn-cert: DFN-CERT-2018-1408 |
| dfn-cert: DFN-CERT-2016-1372 |
| dfn-cert: DFN-CERT-2016-1164 |
| dfn-cert: DFN-CERT-2016-0388 |
| dfn-cert: DFN-CERT-2015-1853 |
| dfn-cert: DFN-CERT-2015-1332 |
| dfn-cert: DFN-CERT-2015-0884 |
| dfn-cert: DFN-CERT-2015-0800 |
| dfn-cert: DFN-CERT-2015-0758 |
| dfn-cert: DFN-CERT-2015-0567 |
| dfn-cert: DFN-CERT-2015-0544 |
| dfn-cert: DFN-CERT-2015-0530 |
| dfn-cert: DFN-CERT-2015-0396 |
| dfn-cert: DFN-CERT-2015-0375 |
| dfn-cert: DFN-CERT-2015-0374 |
| dfn-cert: DFN-CERT-2015-0305 |
| dfn-cert: DFN-CERT-2015-0199 |
| dfn-cert: DFN-CERT-2015-0079 |
| dfn-cert: DFN-CERT-2015-0021 |
| dfn-cert: DFN-CERT-2014-1414 |
| dfn-cert: DFN-CERT-2013-1847 |
| dfn-cert: DFN-CERT-2013-1792 |
| dfn-cert: DFN-CERT-2012-1979 |
| dfn-cert: DFN-CERT-2012-1829 |
| dfn-cert: DFN-CERT-2012-1530 |
| dfn-cert: DFN-CERT-2012-1380 |
| dfn-cert: DFN-CERT-2012-1377 |
| dfn-cert: DFN-CERT-2012-1292 |
| dfn-cert: DFN-CERT-2012-1214 |
| dfn-cert: DFN-CERT-2012-1213 |
| dfn-cert: DFN-CERT-2012-1180 |
| dfn-cert: DFN-CERT-2012-1156 |
| dfn-cert: DFN-CERT-2012-1155 |
| dfn-cert: DFN-CERT-2012-1039 |
| dfn-cert: DFN-CERT-2012-0956 |
| dfn-cert: DFN-CERT-2012-0908 |
| dfn-cert: DFN-CERT-2012-0868 |
| dfn-cert: DFN-CERT-2012-0867 |
| dfn-cert: DFN-CERT-2012-0848 |
| dfn-cert: DFN-CERT-2012-0838 |
| dfn-cert: DFN-CERT-2012-0776 |
| dfn-cert: DFN-CERT-2012-0722 |
| dfn-cert: DFN-CERT-2012-0638 |
| dfn-cert: DFN-CERT-2012-0627 |
| dfn-cert: DFN-CERT-2012-0451 |
| dfn-cert: DFN-CERT-2012-0418 |
| dfn-cert: DFN-CERT-2012-0354 |

```
dfn-cert:  DFN-CERT-2012-0234
dfn-cert:  DFN-CERT-2012-0221
dfn-cert:  DFN-CERT-2012-0177
dfn-cert:  DFN-CERT-2012-0170
dfn-cert:  DFN-CERT-2012-0146
dfn-cert:  DFN-CERT-2012-0142
dfn-cert:  DFN-CERT-2012-0126
dfn-cert:  DFN-CERT-2012-0123
dfn-cert:  DFN-CERT-2012-0095
dfn-cert:  DFN-CERT-2012-0051
dfn-cert:  DFN-CERT-2012-0047
dfn-cert:  DFN-CERT-2012-0021
dfn-cert:  DFN-CERT-2011-1953
dfn-cert:  DFN-CERT-2011-1946
dfn-cert:  DFN-CERT-2011-1844
dfn-cert:  DFN-CERT-2011-1826
dfn-cert:  DFN-CERT-2011-1774
dfn-cert:  DFN-CERT-2011-1743
dfn-cert:  DFN-CERT-2011-1738
dfn-cert:  DFN-CERT-2011-1706
dfn-cert:  DFN-CERT-2011-1628
dfn-cert:  DFN-CERT-2011-1627
dfn-cert:  DFN-CERT-2011-1619
dfn-cert:  DFN-CERT-2011-1482
```

[ return to 106.3.18.183 ]

This file was automatically generated.